



# GigaVUE Firewall Security Guide

**GigaVUE**

Product Version: 6.2

Document Version: 1.0

Last Updated: Wednesday, February 15, 2023

(See Change Notes for document updates.)

**Copyright 2023 Gigamon Inc.. All rights reserved.**

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc..

**Trademark Attributions**

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at [www.gigamon.com/legal-trademarks](http://www.gigamon.com/legal-trademarks). All other trademarks are the trademarks of their respective owners.

Gigamon Inc.  
3300 Olcott Street  
Santa Clara, CA 95054  
408.831.4000

# Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Document Version	Date Updated	Change Notes
1.0	02/15/2022	The original release of this document with 6.2 GA

# Contents

<b>GigaVUE Firewall Security Guide</b> .....	<b>1</b>
Change Notes .....	2
Contents .....	3
Audience .....	4
Get started with GigaVUE Security .....	4
Open Ports in GigaVUE-FM .....	5
Open Default Ports .....	5
Open Ports for GigaVUE-FM Migration .....	7
Open Ports for High Availability .....	8
Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster .....	9
Open Ports in GigaVUE HC Series Devices .....	10
Open Ports in GigaVUE G Series Devices .....	12
Open Ports for Clustered Node Communication .....	12
Open Default Ports .....	13
Open Ports for GigaVUE-FM Migration .....	14
Open Ports for High Availability .....	15
Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster .....	17
Open Ports in GigaVUE HC Series Devices .....	17
Open Ports in GigaVUE G Series Devices .....	19
Open Ports for Clustered Node Communication .....	19
Network Firewall Requirements for VMware .....	20
Network Firewall Requirements for ESXi .....	20
Network Firewall Requirements for NSX-T .....	21
Network Firewall Requirements for OpenStack .....	23
Network Firewall Requirements for Azure .....	25
Network Security Groups for Azure (V Series 1) .....	27
Network Security Groups for GigaVUE V Series 1 Node .....	27
Network Requirements for Gigamon Containerized Broker (GCB) .....	28
Network Firewall Requirements for Nutanix .....	29
Network Firewall Requirements for Universal Container Tap .....	31
Network Firewall Requirements for Gigamon Containerized Box .....	31
Security Group for AWS (V Series 1) .....	32
.....	33
Security Group for AWS (V Series 2) .....	33

Security Group for OpenStack (V Series 1) .....	35
Additional Sources of Information .....	38
Documentation .....	38
Documentation Feedback .....	41
Contact Technical Support .....	42
Contact Sales .....	42
The VUE Community .....	43
<b>Glossary .....</b>	<b>44</b>

## Audience

This guide is intended for the users who have basic understanding of VMs and Nutanix Environment. This document expects the users to be familiar with the following terminologies that are used in this guide:

- **Cluster:** A group of nodes.
- **Node:** A node is a working machine in Nutanix cluster. Each node runs a standard hypervisor with processors, memories, and local storages.

## Get started with GigaVUE Security

This guide provides information about the open ports in GigaVUE-FM, GigaVUE-FM High Availability, open ports in GigaVUE-H series devices, open ports in GigaVUE-G series devices, open ports in GigaVUE HC Series and GigaVUE TA Series devices.

You can also get information about the Network Firewall Requirements for V Series 2 node deployment, OpenStack, V Series 1 configuration, Gigamon fabrics for Nutanix deployments, Kubernetes network requirements for GCB.

Topics:

- [Open Ports in GigaVUE-FM](#)
- [Network Firewall Requirements for VMware](#)
- [Network Firewall Requirements for OpenStack](#)
- [Network Firewall Requirements for Azure](#)
- [Network Security Groups for Azure \(V Series 1\)](#)
- [Network Requirements for Gigamon Containerized Broker \(GCB\)](#)
- [Network Firewall Requirements for Nutanix](#)
- [Security Group for AWS \(V Series 1\)](#)

- [Security Group for AWS \(V Series 2\)](#)
- [Security Group for OpenStack \(V Series 1\)](#)
- [Security Group](#)

## Open Ports in GigaVUE-FM

This appendix provides information about the open ports in GigaVUE-FM and also in the devices. Refer to the following sections:

- [Open Default Ports](#)
- [Open Ports for GigaVUE-FM Migration](#)
- [Open Ports for High Availability](#)
- [Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster](#)
- [Open Ports in GigaVUE HC Series Devices](#)
- [Open Ports in GigaVUE G Series Devices](#)
- [Open Ports for Clustered Node Communication](#)

### Open Default Ports

The following table provides information about the default ports open in the firewall for GigaVUE-FM. The table is sorted by Protocol and then Port Number.

Port Number	Protocol	Service	Traffic Direction	Description
80	HTTP	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for redirecting the traffic internally to port 443. <b>Note:</b> You can choose to shut down port 80 for enhanced security.
443	HTTPS	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for normal GigaVUE-FM user interaction.

Port Number	Protocol	Service	Traffic Direction	Description
			Bidirectional traffic between GigaVUE-FM and GigaVUE-VM.	
389	LDAP	AAA	Bidirectional traffic between LDAP server and GigaVUE-FM	Used for accessing and maintaining distributed directory information services over the Internet Protocol (IP) network.
636	LDAP	AAA	Bidirectional traffic between LDAP server and GigaVUE-FM	Used for secure LDAP protocol over SSL for accessing and maintaining distributed directory information services over the Internet Protocol (IP) network.
1812/1813 1645/1646	Radius	AAA	Bidirectional traffic between Radius server and GigaVUE-FM	Used for running the client/server protocol in the application layer. They can use either TCP or UDP as the transport protocol.
49	TACACS	AAA	Bidirectional traffic between TACACS server and GigaVUE-FM	Used for communicating with the authentication server in order to determine if you have access to the network.
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	<ul style="list-style-type: none"> <li>Used for GigaVUE-FM admin user login. Also, used for initial GigaVUE-FM IP configuration.</li> <li>Used by the web browser to communicate with GigaVUE-VM for troubleshooting purposes.</li> </ul>
514	TCP	Logstash	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending device log messages via SSL from devices to GigaVUE-FM.
5672	TCP	RabbitMq	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
5671	TCP/SSL	RabbitMq	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
53	UDP	DNS	Bidirectional traffic between a DNS server and GigaVUE-FM	Used to resolve Fully Qualified Domain Names (FQDNs).
68	UDP	DHCP	Bidirectional traffic between GigaVUE-FM and DHCP server	Used only if DHCP is enabled on the GigaVUE-FM appliance.

Port Number	Protocol	Service	Traffic Direction	Description
123	UDP	NTP	Bidirectional traffic between a Network Time Protocol (NTP) server and GigaVUE-FM	Used only if GigaVUE-FM is configured to use NTP.
162	UDP	SNMP	Unidirectional traffic from managed appliances to GigaVUE-FM	Used to process incoming traps sent from managed appliances to GigaVUE-FM.
2055	UDP	NetFlow	Unidirectional traffic from managed Appliances to GigaVUE-FM	Used for receiving NetFlow traffic.
2056	UDP	NetFlow	Unidirectional traffic from physical nodes to GigaVUE-FM	Used by Application Intelligence for sending monitoring reports to GigaVUE-FM

### Open Ports for GigaVUE-FM Migration

The following table provides details about ports that must be open during GigaVUE-FM migration.

Port Number	Protocol	Service	Traffic Direction	Description
443	HTTPS	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for API and GUI access related operations.
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	Used for transferring configuration files between two instances of GigaVUE-FM.
902	TCP/UDP	ESXi Host	Bidirectional traffic between VMware vCenter and ESXi hosts	<ul style="list-style-type: none"> <li>For migration and provisioning purposes, this port must be open between the VMware vCenter server and the VMware ESXi hosts. Otherwise, GigaVUE-FM bulk deployment fails.</li> <li>Used for sending data from</li> </ul>

Port Number	Protocol	Service	Traffic Direction	Description
				vCenter Server to the ESXi host. The ESXi host uses this port to send regular heartbeat to the vCenter Server system.

### Open Ports for High Availability

The following table provides details about ports that must be open for GigaVUE-FM High Availability.

Port Number	Protocol	Service	Traffic Direction	Description
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	<ul style="list-style-type: none"> <li>Used for GigaVUE-FM admin user login. Also, used for initial GigaVUE-FM IP configuration.</li> <li>Used by the web browser to communicate with GigaVUE-VM for troubleshooting purposes.</li> <li>Used for transferring configuration files between two GigaVUE-FM instances during migration.</li> </ul>
80	TCP	HTTP	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for redirecting the traffic internally to port 443. <b>Note:</b> You can choose to shut down port 80 for enhanced security.
443	TCP	HTTPS	<ul style="list-style-type: none"> <li>Bidirectional traffic between Web Browser and GigaVUE-FM.</li> <li>Bidirectional traffic between GigaVUE-FM and GigaVUE-VM.</li> </ul>	Used for normal GigaVUE-FM user interaction.



Port Number	Protocol	Service	Traffic Direction	Description
			<ul style="list-style-type: none"> <li>Bidirectional traffic between the GigaVUE-FM instances in a High Availability group.</li> </ul>	
514	TCP/UDP	Shell/Syslog	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending device log messages via SSL from devices to GigaVUE-FM.
4369	TCP	EPMD/RMQ	Bidirectional traffic between RMQ members in cluster.	Small additional process that runs alongside every RabbitMQ node and is used by the runtime to discover what port a particular node listens to. The port is then used by peer nodes.
5671	TCP	amqps	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
25672	TCP	RabbitMQ/ SNMP Traps	Bidirectional traffic between RMQ members in cluster.	
68	UDP	DHCP	Bidirectional traffic between GigaVUE-FM and DHCP server	Used only if DHCP is enabled on the GigaVUE-FM appliance.
162	UDP	SNMP	Unidirectional traffic from managed appliances to GigaVUE-FM	Used to process incoming traps sent from managed appliances to GigaVUE-FM.

**NOTE:** Ports 9514 and 9162 are used to receive the traffic forwarded by ports 514 and 162, respectively. Therefore, these ports need not be opened explicitly.

## Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster

The following table lists the ports that must be open for communication between the members of GigaVUE-FM High Availability cluster.

**NOTE:** These ports cannot be accessed by standalone GigaVUE-FM instances.

Port Number	Protocol	Service	Traffic Direction	Description
8300	TCP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used To handle incoming requests from other agents.
8301	TCP/UDP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication over LAN.
8302	TCP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication over WAN.
30865	TCP	CSync2	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for Synchronization of files/directories across cluster. For example, Image files during GigaVUE-FM HA Upgrade.
9300	TCP	Elastic Search	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication.
27017	TCP	MongoDB	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for data replication across clusters and data access through GigaVUE-OS CLI.

## Open Ports in GigaVUE HC Series Devices

The following table lists the open ports in GigaVUE-H series devices. GigaVUE-FM manages the devices using these open ports.

Port Number	Protocol	Service	Traffic Direction	Description
22	SSH	Device Management	Bidirectional traffic between GigaVUE-FM and devices.	Used for image download, configuration backup/restore operations
80	HTTP	Communication	Bidirectional traffic between GigaVUE-FM and devices.	Used for initial communication setup. Assumption is that HTTP redirect will be turned ON in all GigaVUE devices and FM will use HTTP(S) henceforth

Port Number	Protocol	Service	Traffic Direction	Description
443	HTTPS	Communication	Bidirectional traffic between GigaVUE-FM and devices.	<p>GigaVUE-FM to device communication. Refer to the following notes:</p> <ul style="list-style-type: none"> <li>Starting in software version 5.9.00, XML Gateway services are shutdown in the devices. Therefore, if you change the HTTPS port number of a device using CLI, then: <ul style="list-style-type: none"> <li>For devices that are not added and managed by GigaVUE-FM: You must update the HTTPS port number when adding the nodes using the Add Physical Nodes page in GigaVUE-FM GUI. Refer to the <i>Add Nodes Manually</i> section for more details.</li> <li>For devices that have already been added and managed by GigaVUE-FM: You must update the HTTPS port number from the Node Details page (<b>Admin &gt; System &gt; Node Details</b>). In the Node Details page, select the device and click <b>Edit</b> to update the port number and click <b>Save</b>.</li> </ul> </li> <li>Failure to do so will terminate communication between the device and GigaVUE-FM</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p><b>NOTE:</b> Until software version 6.2, if the HTTPS port number is changed using CLI, then GigaVUE-FM will learn the port number through the XML Gateway request.</p> </div> <ul style="list-style-type: none"> <li>Devices with software version greater than or equal to software version 5.9.00 are XSRF enabled, by default.</li> </ul>

## Open Ports in GigaVUE G Series Devices

The following table lists the open ports in GigaVUE-G series devices. GigaVUE-FM manages the devices using these open ports.

Port Number	Protocol	Service	Traffic Direction	Description
22	SSH	Device Management	Bidirectional traffic between GigaVUE-FM and devices.	Configuration backup/restore operations
80	HTTP	Communication	Bidirectional traffic between GigaVUE-FM and devices.	Used for initial communication setup. Assumption is that HTTP redirect will be turned ON in all GigaVUE devices and FM will use HTTP(S) henceforth
443	HTTPS	Communication	Bidirectional traffic between GigaVUE-FM and devices.	GigaVUE-FM to device communication

## Open Ports for Clustered Node Communication

The following table lists the open ports in GigaVUE HC Series and GigaVUE TA Series devices.

Port Number	Protocol	Service	Traffic Direction	Description
5353	UDP	Communication	Bidirectional	Used for cluster communication
6379	TCP	Communication	Bidirectional	Used to communicate with clients that need to reach the cluster nodes

This appendix provides information about the open ports in GigaVUE-FM and also in the devices. Refer to the following sections:

- [Open Default Ports](#)
- [Open Ports for GigaVUE-FM Migration](#)
- [Open Ports for High Availability](#)

- [Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster](#)
- [Open Ports in GigaVUE HC Series Devices](#)
- [Open Ports in GigaVUE G Series Devices](#)
- [Open Ports for Clustered Node Communication](#)

## Open Default Ports

The following table provides information about the default ports open in the firewall for GigaVUE-FM. The table is sorted by Protocol and then Port Number.

Port Number	Protocol	Service	Traffic Direction	Description
80	HTTP	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for redirecting the traffic internally to port 443. <b>Note:</b> You can choose to shut down port 80 for enhanced security.
443	HTTPS	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM Bidirectional traffic between GigaVUE-FM and GigaVUE-VM.	Used for normal GigaVUE-FM user interaction.
389	LDAP	AAA	Bidirectional traffic between LDAP server and GigaVUE-FM	Used for accessing and maintaining distributed directory information services over the Internet Protocol (IP) network.
636	LDAP	AAA	Bidirectional traffic between LDAP server and GigaVUE-FM	Used for secure LDAP protocol over SSL for accessing and maintaining distributed directory information services over the Internet Protocol (IP) network.
1812/1813 1645/1646	Radius	AAA	Bidirectional traffic between Radius server and GigaVUE-FM	Used for running the client/server protocol in the application layer. They can use either TCP or UDP as the transport protocol.
49	TACACS	AAA	Bidirectional traffic between TACACS server and GigaVUE-FM	Used for communicating with the authentication server in order to determine if you have access to the network.
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	<ul style="list-style-type: none"> <li>● Used for GigaVUE-FM admin user login. Also, used for initial GigaVUE-FM IP configuration.</li> </ul>

Port Number	Protocol	Service	Traffic Direction	Description
				<ul style="list-style-type: none"> <li>Used by the web browser to communicate with GigaVUE-VM for troubleshooting purposes.</li> </ul>
514	TCP	Logstash	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending device log messages via SSL from devices to GigaVUE-FM.
5672	TCP	RabbitMq	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
5671	TCP/SSL	RabbitMq	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
53	UDP	DNS	Bidirectional traffic between a DNS server and GigaVUE-FM	Used to resolve Fully Qualified Domain Names (FQDNs).
68	UDP	DHCP	Bidirectional traffic between GigaVUE-FM and DHCP server	Used only if DHCP is enabled on the GigaVUE-FM appliance.
123	UDP	NTP	Bidirectional traffic between a Network Time Protocol (NTP) server and GigaVUE-FM	Used only if GigaVUE-FM is configured to use NTP.
162	UDP	SNMP	Unidirectional traffic from managed appliances to GigaVUE-FM	Used to process incoming traps sent from managed appliances to GigaVUE-FM.
2055	UDP	NetFlow	Unidirectional traffic from managed Appliances to GigaVUE-FM	Used for receiving NetFlow traffic.
2056	UDP	NetFlow	Unidirectional traffic from physical nodes to GigaVUE-FM	Used by Application Intelligence for sending monitoring reports to GigaVUE-FM

### Open Ports for GigaVUE-FM Migration

The following table provides details about ports that must be open during GigaVUE-FM migration.

Port Number	Protocol	Service	Traffic Direction	Description
443	HTTPS	GigaVUE-FM GUI	Bidirectional traffic between Web Browser and GigaVUE-FM	Used for API and GUI access related operations.
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	Used for transferring configuration files between two instances of GigaVUE-FM.
902	TCP/UDP	ESXi Host	Bidirectional traffic between VMware vCenter and ESXi hosts	<ul style="list-style-type: none"> <li>For migration and provisioning purposes, this port must be open between the VMware vCenter server and the VMware ESXi hosts. Otherwise, GigaVUE-FM bulk deployment fails.</li> <li>Used for sending data from vCenter Server to the ESXi host. The ESXi host uses this port to send regular heartbeat to the vCenter Server system.</li> </ul>

### Open Ports for High Availability

The following table provides details about ports that must be open for GigaVUE-FM High Availability.

Port Number	Protocol	Service	Traffic Direction	Description
22	TCP	SSH	Bidirectional traffic between Putty and GigaVUE-FM	<ul style="list-style-type: none"> <li>Used for GigaVUE-FM admin user login. Also, used for initial GigaVUE-FM IP configuration.</li> <li>Used by the web browser to communicate with GigaVUE-VM for troubleshooting purposes.</li> <li>Used for transferring configuration files between two GigaVUE-FM instances during migration.</li> </ul>
80	TCP	HTTP	Bidirectional traffic between Web Browser and	Used for redirecting the traffic internally to port 443.

Port Number	Protocol	Service	Traffic Direction	Description
			GigaVUE-FM	<b>Note:</b> You can choose to shut down port 80 for enhanced security.
443	TCP	HTTPS	<ul style="list-style-type: none"> <li>• Bidirectional traffic between Web Browser and GigaVUE-FM.</li> <li>• Bidirectional traffic between GigaVUE-FM and GigaVUE-VM.</li> <li>• Bidirectional traffic between the GigaVUE-FM instances in a High Availability group.</li> </ul>	Used for normal GigaVUE-FM user interaction.
514	TCP/UDP	Shell/Syslog	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending device log messages via SSL from devices to GigaVUE-FM.
4369	TCP	EPMD/RMQ	Bidirectional traffic between RMQ members in cluster.	Small additional process that runs alongside every RabbitMQ node and is used by the runtime to discover what port a particular node listens to. The port is then used by peer nodes.
5671	TCP	amqps	Unidirectional traffic from physical nodes to GigaVUE-FM	Used for sending event notifications via SSL from devices to GigaVUE-FM.
25672	TCP	RabbitMQ/ SNMP Traps	Bidirectional traffic between RMQ members in cluster.	
68	UDP	DHCP	Bidirectional traffic between GigaVUE-FM and DHCP server	Used only if DHCP is enabled on the GigaVUE-FM appliance.
162	UDP	SNMP	Unidirectional traffic from managed appliances to GigaVUE-FM	Used to process incoming traps sent from managed appliances to GigaVUE-FM.

**NOTE:** Ports 9514 and 9162 are used to receive the traffic forwarded by ports 514 and 162, respectively. Therefore, these ports need not be opened explicitly.



## Open Ports for Communication Between Members of GigaVUE-FM High Availability Cluster

The following table lists the ports that must be open for communication between the members of GigaVUE-FM High Availability cluster.

**NOTE:** These ports cannot be accessed by standalone GigaVUE-FM instances.

Port Number	Protocol	Service	Traffic Direction	Description
8300	TCP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used To handle incoming requests from other agents.
8301	TCP/UDP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication over LAN.
8302	TCP	Consul	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication over WAN.
30865	TCP	CSync2	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for Synchronization of files/directories across cluster. For example, Image files during GigaVUE-FM HA Upgrade.
9300	TCP	Elastic Search	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for inter-cluster communication.
27017	TCP	MongoDB	Bidirectional traffic between members in GigaVUE-FM cluster.	Used for data replication across clusters and data access through GigaVUE-OS CLI.

## Open Ports in GigaVUE HC Series Devices

The following table lists the open ports in GigaVUE-H series devices. GigaVUE-FM manages the devices using these open ports.

Port Number	Protocol	Service	Traffic Direction	Description
22	SSH	Device Management	Bidirectional traffic between GigaVUE-FM and devices.	Used for image download, configuration backup/restore operations
80	HTTP	Communication	Bidirectional traffic between GigaVUE-FM and devices.	Used for initial communication setup. Assumption is that HTTP redirect will be turned ON in all GigaVUE devices and FM will use HTTP(S) henceforth
443	HTTPS	Communication	Bidirectional traffic between GigaVUE-FM and devices.	GigaVUE-FM to device communication. Refer to the following notes: <ul style="list-style-type: none"> <li>Starting in software version 5.9.00, XML Gateway services are shutdown in the devices. Therefore, if you change the HTTPS port number of a device using CLI, then: <ul style="list-style-type: none"> <li>For devices that are not added and managed by GigaVUE-FM: You must update the HTTPS port number when adding the nodes using the Add Physical Nodes page in GigaVUE-FM GUI. Refer to the <i>Add Nodes Manually</i> section for more details.</li> <li>For devices that have already been added and managed by GigaVUE-FM: You must update the HTTPS port number from the Node Details page (<b>Admin &gt; System &gt; Node Details</b>). In the Node Details page, select the device and click <b>Edit</b> to update the port number and click <b>Save</b>.</li> </ul> </li> </ul>

Port Number	Protocol	Service	Traffic Direction	Description
				<ul style="list-style-type: none"> <li>Failure to do so will terminate communication between the device and GigaVUE-FM</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>NOTE:</b> Until software version 6.2, if the HTTPS port number is changed using CLI, then GigaVUE-FM will learn the port number through the XML Gateway request.</p> </div> <ul style="list-style-type: none"> <li>Devices with software version greater than or equal to software version 5.9.00 are XSRF enabled, by default.</li> </ul>

### Open Ports in GigaVUE G Series Devices

The following table lists the open ports in GigaVUE-G series devices. GigaVUE-FM manages the devices using these open ports.

Port Number	Protocol	Service	Traffic Direction	Description
22	SSH	Device Management	Bidirectional traffic between GigaVUE-FM and devices.	Configuration backup/restore operations
80	HTTP	Communication	Bidirectional traffic between GigaVUE-FM and devices.	Used for initial communication setup. Assumption is that HTTP redirect will be turned ON in all GigaVUE devices and FM will use HTTP(S) henceforth
443	HTTPS	Communication	Bidirectional traffic between GigaVUE-FM and devices.	GigaVUE-FM to device communication

### Open Ports for Clustered Node Communication

The following table lists the open ports in GigaVUE HC Series and GigaVUE TA Series devices.

Port Number	Protocol	Service	Traffic Direction	Description
5353	UDP	Communication	Bidirectional	Used for cluster communication
6379	TCP	Communication	Bidirectional	Used to communicate with clients that need to reach the cluster nodes

## Network Firewall Requirements for VMware

This section consist of following topics:

- [Network Firewall Requirements for ESXi](#)
- [Network Firewall Requirements for NSX-T](#)

### Network Firewall Requirements for ESXi

Following are the Network Firewall Requirements for V Series 2 node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts vCenter	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts to import the V Series OVA files
GigaVUE-FM	V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with V Series node
GigaVUE-FM	V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE V Series 2 Nodes to send traffic health

						updates to GigaVUE-FM	
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM	
			22		ssh		
Remote Source	V Series Nodes	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes (Applicable for Tunnel Ingress option only)	
			N/A		IP 47		GRE
			4754		UDP		UDPGRE
V Series Nodes	Tool/ HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows V Series node to communicate and tunnel traffic to the Tool	
			N/A		IP 47		GRE
V Series Nodes	Tool/ HC Series instance	N/A	N/A	ICMP	Echo Request	Allows V Series node to health check tunnel destination traffic (Optional)	
					Echo Response		
V Series Nodes	GigaVUE-FM	Any (1024-65535)	Any (1024-65535)	TCP	Custom TCP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM	

## Network Firewall Requirements for NSX-T

Following are the Network Firewall Requirements for V Series 2 node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter, NSX-T and all ESXi hosts.
	NSX-T Manager					
	vCenter					
GigaVUE FM	V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with V Series node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
GigaVUE-FM	V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM
Remote Source	V Series Nodes	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
V Series Nodes	Tool/ HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows V Series node to communicate and tunnel traffic to the Tool
			N/A	IP 47	GRE	
V Series Nodes	Tool/ HC Series instance	N/A	N/A	ICMP	echo Request	Allows V Series node to health check tunnel destination traffic (Optional)
					echo Response	

GigaVUE-FM	V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM
GigaVUE-FM	External Image Server URL	Any (1024-65535)	Custom port on web Server	TCP	http	Access to image server to image lookup and checks, and downloading the image
NSX-T Manager						
vCenter						

## Network Firewall Requirements for OpenStack

Following are the Network Firewall Requirements for OpenStack.

Direction	Ether Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	HTTPS	TCP	443	Any IP address	Allows users to connect to the GigaVUE-FM GUI.
Inbound	IPv4	UDP	53	Any IP address	Allows GigaVUE-FM to communicate with standard DNS server
Inbound	Custom TCP Rule	TCP	5671	V Series 2 Node IP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation G-vTAP Agents to send statistics to GigaVUE-FM.
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with V Series node
<b>G-vTAP Controller</b>					
Inbound	Custom	TCP	9900	Custom	Allows GigaVUE-FM to

Direction	Ether Type	Protocol	Port	CIDR	Purpose
	TCP Rule			GigaVUE-FM IP	communicate with G-vTAP Controllers
<b>G-vTAP Agent</b>					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP Controller IP	Allows G-vTAP Controllers to communicate with G-vTAP Agents
<b>G-vTAP OVS Controller</b>					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP OVS Controllers
<b>G-vTAP OVS Agent</b>					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP OVS Controller IP	Allows G-vTAP OVS Controllers to communicate with G-vTAP OVS Agents
<b>GigaVUE V Series Proxy</b>					
Inbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxys.
Outbound	Custom TCP Rule	TCP	8889	V Series 2 node IP	Allows V Series Proxy to communicate with V Series node
<b>GigaVUE V Series 2 Node</b>					
Inbound	Custom TCP Rule	TCP(6)	8889	GigaVUE V Series Proxy IP address	Allows GigaVUE V Series Proxys to communicate with GigaVUE V Series nodes
Outbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE V Series Node to communicate with GigaVUE V Series Proxy
Outbound	Custom UDP Rule	UDP	<ul style="list-style-type: none"> <li>● VXLAN (default 4789)</li> <li>● L2GRE (IP 47)</li> </ul>	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM



Network	Purpose
<b>Management</b>	Identify the subnets that GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
<b>Data</b>	Identify the subnets that receives the mirrored tunnel traffic from the monitored instances. In data network, if a tool subnet is selected then the V Series node egress traffic on to the destinations or tools.

**NOTE:** If you are using IPv6 in the tenant network, then it is recommended to use SLAAC or stateless DHCPv6 for dynamic address assignment.

## Network Firewall Requirements for Azure

Following is the Network Firewall Requirements for V Series 2 node deployment.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	<ul style="list-style-type: none"> <li>• HTTPS</li> <li>• SSH</li> </ul>	TCP	<ul style="list-style-type: none"> <li>• 443</li> <li>• 22</li> </ul>	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	Custom TCP Rule	TCP	5671	V Series 2 Node IP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation G-vTAP Agents to send statistics to GigaVUE-FM.
Outbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
<b>G-vTAP Controller</b>					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM

Direction	Type	Protocol	Port	CIDR	Purpose
Outbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Controller to communicate with G-vTAP Agents
<b>G-vTAP Agent</b>					
Inbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Agents to communicate with G-vTAP Controller
Outbound	<ul style="list-style-type: none"> <li>• UDP</li> <li>• IP</li> </ul>	<ul style="list-style-type: none"> <li>• UDP (VXLAN)</li> <li>• IP Protocol (L2GRE)</li> </ul>	VXLAN (default 4789)	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
<b>V Series Proxy (optional)</b>					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 node IP	Allows V Series Proxy to communicate with V Series node
<b>V Series 2 node</b>					
Inbound	Custom TCP Rule	TCP	8889	<ul style="list-style-type: none"> <li>• GigaVUE-FM IP</li> <li>• V Series Proxy IP</li> </ul>	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node
Inbound	<ul style="list-style-type: none"> <li>• UDP</li> <li>• IP</li> </ul>	<ul style="list-style-type: none"> <li>• UDP (VXLAN)</li> <li>• IP Protocol (L2GRE)</li> </ul>	<ul style="list-style-type: none"> <li>• VXLAN (default 4789)</li> <li>• L2GRE</li> </ul>	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes

Direction	Type	Protocol	Port	CIDR	Purpose
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	Custom UDP Rule	<ul style="list-style-type: none"> <li>• UDP (VXLAN)</li> <li>• IP Protocol (L2GRE)</li> </ul>	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	<ul style="list-style-type: none"> <li>• echo request</li> <li>• echo reply</li> </ul>	Tool IP	Allows V Series node to health check tunnel destination traffic

## Network Security Groups for Azure (V Series 1)

### Network Security Groups for GigaVUE V Series 1 Node

Following are the Network Firewall Requirements for V Series 1 configuration.

Direction	Ether Type	Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
<b>GigaVUE-FM Inside Azure</b>					
Inbound	HTTPS	TCP(6)	443	Anywhere Any IP	Allows G-vTAP Controllers, GigaVUE V Series Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
<b>G-vTAP Controller</b>					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP Controllers

Direction	Ether Type	Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
<b>G-vTAP Agent</b>					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP Controller IP	Allows G-vTAP Controllers to communicate with G-vTAP Agents
<b>GigaVUE V Series Controller</b>					
Inbound	Custom TCP Rule	TCP	9902	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Controllers
<b>GigaVUE V Series 1 node</b>					
Inbound	Custom TCP Rule	TCP	9903	Custom GigaVUE V Series Controller IP	Allows GigaVUE V Series Controllers to communicate with GigaVUE V Series nodes
<b>VXLAN Traffic</b>					
Inbound	Custom UDP Rule	VXLAN	4789		Allows mirrored traffic from G-vTAP Agents to be sent to GigaVUE V Series nodes using VXLAN tunnel Allows monitored traffic to be sent from GigaVUE V Series nodes to the tools using VXLAN tunnel

## Network Requirements for Gigamon Containerized Broker (GCB)

The following table describes the Kubernetes network requirements for GCB to work efficiently.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>Gigamon Containerized Broker</b> deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM

Direction	Type	Protocol	Port	CIDR	Purpose
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with GCB Controller.
Outbound	HTTPS	TCP	42042	Any IP address	Allows GCB to communicate with GigaVUE-FM to send statistics data.

## Network Firewall Requirements for Nutanix

This section consists of the following topics:

- [Network Firewall Requirements for Nutanix \(V Series 1\)](#)
- [Network Firewall Requirements for Nutanix \(V Series 2\)](#)

### Network Firewall Requirements for Nutanix (V Series 1)

Following are the Network Firewall Requirements for Gigamon fabrics for Nutanix deployments.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM Inside Nutanix</b>					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allow GVMs, GigaVUE Cloud Suite fabric controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allow GVMs, GigaVUE Cloud Suite fabric controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP	9902	GigaVUE Cloud Suite Fabric Controller IP	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite Fabric Controllers IP.
<b>GigaVUE Cloud Suite Fabric Controller</b>					
Inbound	Custom TCP Rule	TCP	9902	GigaVUE-FM IP	Allows GVM to communicate with

Direction	Type	Protocol	Port	CIDR	Purpose
					GigaVUE Cloud Suite Fabric Controllers.
Outbound	Custom TCP Rule	TCP	9903	GVM IP Subnet	Allows GigaVUE Cloud Suite Fabric Controller to communicate with GVMs.
<b>GVM</b>					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE Cloud Suite Fabric Controller IP	Allows GigaVUE Cloud Suite Fabric Controller IP to communicate with GVMs.
Outbound	Custom UDP Rule	UDP	<ul style="list-style-type: none"> <li>VXLAN (default 4789)</li> <li>L2GRE (IP 47)</li> </ul>	Tool IP	Allows GVM to communicate and tunnel traffic to the tool
Outbound	Custom ICMP Rule	ICMP	-	Tool IP	Allows GVM to health check the tool traffic.

## Network Firewall Requirements for Nutanix (V Series 2)

Following are the Network Firewall Requirements for Gigamon fabrics for Nutanix deployments.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP	9902	GigaVUE V SeriesProxy IP	Allows GigaVUE-FM to communicate with GigaVUE V SeriesProxy.
<b>GigaVUE V Series Node</b>					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE V SeriesProxy	Allows GigaVUE V Series Proxy to communicate

Direction	Type	Protocol	Port	CIDR	Purpose
				IP	with GigaVUE® V Series Nodes
Outbound	Custom UDP Rule	UDP	<ul style="list-style-type: none"> <li>VXLAN (default 4789)</li> <li>L2GRE (IP 47)</li> </ul>	Tool IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound	Custom ICMP Rule	ICMP	-	Tool IP	Allows GigaVUE® V Series Node to health check the tool traffic

## Network Firewall Requirements for Universal Container Tap

Following are the Network Firewall Requirements for Universal Container Tap (UCT).

Direction	Type	Protocol	Port	CIDR	Purpose
<b>Universal Container Tap</b> deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows UCT Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with UCT Controller.
Outbound	HTTPS	TCP	42042	Any IP address	Allows GigaVUE-FM to communicate with UCT to send statistical data.

## Network Firewall Requirements for Gigamon Containerized Box

Following are the Network Firewall Requirements for Gigamon Containerized Box (GCB).

Direction	Type	Protocol	Port	CIDR	Purpose
<b>Gigamon Containerized Broker</b> deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with GCB

Direction	Type	Protocol	Port	CIDR	Purpose
					Controller.
Outbound	HTTPS	TCP	42042	Any IP address	Allows GCB to communicate with GigaVUE-FM to send statistics data.

## Security Group for AWS (V Series 1)

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE V Series Controllers, GigaVUE V Series nodes, and G-vTAP Controllers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

To create a security group, refer to [Create a security group](#) topic in the AWS Documentation.

It is recommended to create a separate security group for each component using the rules and port numbers listed in the following table.

Direction	Type	Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
<b>GigaVUE-FM Inside AWS</b>					
Inbound	HTTPS	TCP(6)	443	Anywhere Any IP	Allows G-vTAP Controllers, GigaVUE V Series Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
<b>G-vTAP Controller</b>					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP Controllers
<b>G-vTAP Agent</b>					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP	Allows G-vTAP Controllers to communicate with G-vTAP



Direction	Type	Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
				Controller IP	Agents
<b>GigaVUE V Series Controller</b>					
Inbound	Custom TCP Rule	TCP	9902	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Controllers
<b>GigaVUE V Series 1 node</b>					
Inbound	Custom TCP Rule	TCP	9903	Custom GigaVUE V Series Controller IP	Allows GigaVUE V Series Controllers to communicate with GigaVUE V Series nodes
<b>VXLAN Traffic</b>					
Inbound	Custom UDP Rule	VXLAN	4789		Allows mirrored traffic from G-vTAP Agents to be sent to GigaVUE V Series nodes using VXLAN tunnel Allows monitored traffic to be sent from GigaVUE V Series nodes to the tools using VXLAN tunnel

## Security Group for AWS (V Series 2)

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE V Series Proxies, GigaVUE V Series nodes, and G-vTAP Controllers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

To create a security group, refer to [Create a security group](#) topic in the AWS Documentation.

It is recommended to create a separate security group for each component using the rules and port numbers listed in the following table.

Following is the Network Firewall Requirements for V Series 2 node deployment.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	<ul style="list-style-type: none"> <li>• HTTPS</li> <li>• SSH</li> </ul>	TCP	<ul style="list-style-type: none"> <li>• 443</li> <li>• 22</li> </ul>	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	Custom TCP Rule	TCP	5671	V Series 2 Node IP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation G-vTAP Agents to send statistics to GigaVUE-FM.
Outbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
<b>G-vTAP Controller</b>					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Controller to communicate with G-vTAP Agents
<b>G-vTAP Agent</b>					
Inbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Agents to communicate with G-vTAP Controller
Outbound	<ul style="list-style-type: none"> <li>• UDP</li> <li>• IP</li> </ul>	<ul style="list-style-type: none"> <li>• UDP (VXLAN)</li> <li>• IP Protocol (L2GRE)</li> </ul>	VXLAN (default 4789)	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
<b>V Series Proxy (optional)</b>					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 node IP	Allows V Series Proxy to communicate with V Series node

Direction	Type	Protocol	Port	CIDR	Purpose
<b>V Series 2 node</b>					
Inbound	Custom TCP Rule	TCP	8889	<ul style="list-style-type: none"> <li>GigaVUE-FM IP</li> <li>V Series Proxy IP</li> </ul>	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node
Inbound	<ul style="list-style-type: none"> <li>UDP</li> <li>IP</li> </ul>	<ul style="list-style-type: none"> <li>UDP (VXLAN)</li> <li>IP Protocol (L2GRE)</li> </ul>	<ul style="list-style-type: none"> <li>VXLAN (default 4789)</li> <li>L2GRE</li> </ul>	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	Custom UDP Rule	<ul style="list-style-type: none"> <li>UDP (VXLAN)</li> <li>IP Protocol (L2GRE)</li> </ul>	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	<ul style="list-style-type: none"> <li>echo request</li> <li>echo reply</li> </ul>	Tool IP	Allows V Series node to health check tunnel destination traffic

## Security Group for OpenStack (V Series 1)

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE V Series Controllers, GigaVUE V Series nodes, and G-vTAP Controllers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

The Security Group Rules table lists the rules and port numbers for each component.

Direction	Ether Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	HTTPS	TCP	443	Any IP address	Allows users to connect to the GigaVUE-FM GUI.

Direction	Ether Type	Protocol	Port	CIDR	Purpose
Inbound	IPv4	UDP	67 and 68	Any IP address	Allows GigaVUE-FM to communicate with DHCP server for assigning IP addresses and other related configuration information such as the subnet mask and default gateway
Inbound	IPv4	UDP	53	Any IP address	Allows GigaVUE-FM to communicate with standard DNS server
<b>G-vTAP Controller</b>					
Inbound	IPv4	TCP	9900	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with G-vTAP Controllers
<b>G-vTAP Agent</b>					
Inbound	IPv4	TCP	9901	G-vTAP Controller IP address	Allows G-vTAP Controllers to communicate with G-vTAP Agents
<b>V Series Controller</b>					
Inbound	IPv4	TCP	9902	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with GigaVUE V Series Controllers.
<b>V Series 1 Node</b>					
Inbound	Custom TCP Rule	TCP(6)	9903	GigaVUE V Series Controller IP address	Allows GigaVUE V Series Controllers to communicate with GigaVUE V Series nodes
<b>GRE Traffic</b>					
Inbound	Custom Protocol Rule	GRE (47)	47	Any IP address	Allows mirrored traffic from G-vTAP Agents to be sent to GigaVUE V Series nodes using the L2 GRE or VXLAN tunnel
Outbound	Custom Protocol Rule	GRE (47)	47	Any IP address	Allows monitored traffic from GigaVUE V Series nodes to be sent to the monitoring tools using the L2 GRE or VXLAN tunnel

Direction	Ether Type	Protocol	Port	CIDR	Purpose
<b>VXLAN Traffic</b>					
Inbound	Custom UDPRule	UDP	4789	Any IP address	Allows mirrored traffic from G-vTAP Agents to be sent to GigaVUE V Series nodes using the VXLAN tunnel
Outbound	Custom UDPRule	UDP	4789	Any IP address	Allows monitored traffic from GigaVUE V Series nodes to be sent to the monitoring tools using the VXLAN tunnel

## Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

### Documentation

This table lists all the guides provided for GigaVUE software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

**NOTE:** In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE 6.2 Hardware and Software Guides
<p><b>DID YOU KNOW?</b> If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing <b>Edit &gt; Advanced Search</b> from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p><b>Hardware</b></p> <p>how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE devices; reference information and specifications for the respective GigaVUE devices</p>
<b>GigaVUE-HC1 Hardware Installation Guide</b>
<b>GigaVUE-HC2 Hardware Installation Guide</b>
<b>GigaVUE-HC3 Hardware Installation Guide</b>
<b>GigaVUE-HC1-Plus Hardware Installation Guide</b>
<b>GigaVUE-TA25E Hardware Installation Guide</b>
<b>GigaVUE-TA200E Hardware Installation Guide</b>
<b>GigaVUE-TA25 Hardware Installation Guide</b>
<b>GigaVUE-TA200 Hardware Installation Guide</b>
<b>GigaVUE-TA400 Hardware Installation Guide</b>

## GigaVUE 6.2 Hardware and Software Guides

**GigaVUE-TA10 Hardware Installation Guide**

**GigaVUE-TA40 Hardware Installation Guide**

**GigaVUE-TA100 Hardware Installation Guide**

**GigaVUE-TA100-CXP Hardware Installation Guide**

**GigaVUE-OS Installation Guide for DELL S4112F-ON**

**G-TAP A Series 2 Installation Guide**

**GigaVUE M Series Hardware Installation Guide**

**GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW**

### Software Installation and Upgrade Guides

**GigaVUE-FM Installation, Migration, and Upgrade Guide**

**GigaVUE-OS Upgrade Guide**

**GigaVUE V Series Migration Guide**

### Fabric Management and Administration Guides

**GigaVUE Administration Guide**

covers both GigaVUE-OS and GigaVUE-FM

**GigaVUE Fabric Management Guide**

how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features

### Cloud Guides

how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms

**\*GigaVUE V Series Applications Guide**

**GigaVUE V Series Quick Start Guide**

**GigaVUE Cloud Suite for AWS—GigaVUE V Series 2 Guide**

**GigaVUE Cloud Suite for Azure—GigaVUE V Series 2 Guide**

**GigaVUE Cloud Suite for OpenStack—GigaVUE V Series 2 Guide**

**\*GigaVUE Cloud Suite for Nutanix Guide—GigaVUE V Series 2 Guide**

**GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide**

**\*GigaVUE Cloud Suite for Third Party Orchestration**

**GigaVUE Cloud Suite for AnyCloud Guide**

## GigaVUE 6.2 Hardware and Software Guides

### Universal Container Tap Guide

### Gigamon Containerized Broker Guide

### GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide

### GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide

### GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide

### GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide

### GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide

## Reference Guides

### GigaVUE-OS CLI Reference Guide

library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices

### GigaVUE-OS Cabling Quick Reference Guide

guidelines for the different types of cables used to connect Gigamon devices

### GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

### GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

## Release Notes

### GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;  
important notes regarding installing and upgrading to this release

**NOTE:** Release Notes are not included in the online documentation.

**NOTE:** Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software & Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

## In-Product Help

### GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.



## How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to [My Gigamon](#). Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

### To download release-specific software, release notes, or older PDFs:

1. Log in to [My Gigamon](#)
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

**NOTE:** My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

## Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to:

[documentationfeedback@gigamon.com](mailto:documentationfeedback@gigamon.com)

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
<b>About You</b>	<b>Your Name</b>	
	<b>Your Role</b>	
	<b>Your Company</b>	
<b>For Online Topics</b>	<b>Online doc link</b>	<i>(URL for where the issue is)</i>
	<b>Topic Heading</b>	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>

<b>For PDF Topics</b>	<b>Document Title</b>	<i>(shown on the cover page or in page header )</i>
	<b>Product Version</b>	<i>(shown on the cover page)</i>
	<b>Document Version</b>	<i>(shown on the cover page)</i>
	<b>Chapter Heading</b>	<i>(shown in footer)</i>
	<b>PDF page #</b>	<i>(shown in footer)</i>
<b>How can we improve?</b>	<b>Describe the issue</b>	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	<b>How can we improve the content?</b> <b>Be as specific as possible.</b>	
	<b>Any other comments?</b>	

## Contact Technical Support

For information about Technical Support: Go to **Settings**  > **Support** > **Contact Support** in GigaVUE-FM.

You can also refer to <https://www.gigamon.com/support-and-services/contact-support> for Technical Support hours and contact information.

Email Technical Support at [support@gigamon.com](mailto:support@gigamon.com).

## Contact Sales

Use the following information to Gigamon channel partner or Gigamon sales representatives.

**Telephone:** +1.408.831.4025

**Sales:** [inside.sales@gigamon.com](mailto:inside.sales@gigamon.com)

**Partners:** [www.gigamon.com/partners.html](http://www.gigamon.com/partners.html)

## Premium Support

Email Gigamon at [inside.sales@gigamon.com](mailto:inside.sales@gigamon.com) for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

## The VÜE Community

The **VÜE Community** is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

**Register today at** [community.gigamon.com](http://community.gigamon.com)

**Questions?** Contact our Community team at [community@gigamon.com](mailto:community@gigamon.com).

# Glossary

## D

---

### decrypt list

need to decrypt (formerly blacklist)

### decryptlist

need to decrypt - CLI Command (formerly blacklist)

### drop list

selective forwarding - drop (formerly blacklist)

## F

---

### forward list

selective forwarding - forward (formerly whitelist)

## L

---

### leader

leader in clustering node relationship (formerly master)

## M

---

### member node

follower in clustering node relationship (formerly slave or non-master)

## N

---

### no-decrypt list

no need to decrypt (formerly whitelist)

**nodecryptlist**

no need to decrypt- CLI Command (formerly whitelist)

**P**

---

**primary source**

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

**R**

---

**receiver**

follower in a bidirectional clock relationship (formerly slave)

**S**

---

**source**

leader in a bidirectional clock relationship (formerly master)